PROPOSED ORGANIZATIONAL STRUCTURE

FOR

INFORMATION SYSTEMS SECURITY GROUP

FIVE YEAR PLAN

I. General

This paper contains the origins of an information systems security structure which permits the Office of Security to adjust to the continuing technological advancements and proliferation of information systems. This is not an attempt to justify the need for such an organization, but rather an effort to depict a structure which will effectively identify and address the information systems security problems of the Agency and its contractors.

Information systems are permeating all segments of government and industry. Our traditional concepts of security are no longer sufficient to provide the access, accountability and need-to-know controls necessary for insuring the security of these systems. It is relatively easy to identify those segments of the Agency and contractor world which require the attention of an organization such as Information Systems Security Group (ISSG). It is more difficult, however to develop and manage an organization which can continue to identify and correct the multiplicity of security problems prevalent in the information processing world.

The method considered most successful in coping with the variety of security problems is the use of Information Systems Security Officers (ISSOs). This method has been actively used in ISSG for the past year with reasonable success. Briefly, the ISSO method gives each officer responsibility for insuring the security of all information processing systems used in each Agency office, contractor facility, or overseas station assigned to him. This responsibility will run the gamut from a computer system to a word processor to a facsimile machine or any other type of information processing equipment. Having total information systems security responsibility forces the ISSO to learn and understand the operation of the component assigned him; thereby enabling him to provide more realistic and timely security support.

It should be remembered that the ISSO concept will be the vehicle for performing the functions of each Branch as outlined in the following pages.

II. Top Secret Control Automated Document System (TSCADS) Branch

The function of this Branch is to provide and maintain an automated system for the Agency, which, when coupled with annual inventories, periodic audits and some manual processing, provides a control system for the Agency's Top Secret Collateral holdings. The proposed structure of this Branch should meet TSCADS requirements over the next five years. The one unknown factor relates to the impact APEX might have upon TSCADS. If APEX causes a substantial increase in TSCADS holdings, it might affect any future structuring of this Branch. The functions of this Branch can logically be divided into three specific areas:

A. Data Input and Control

This is the heart of the TSCADS program. Maintaining a current data base involves the daily input, via remote terminal, of numerous document control numbers. The data base now contains 180,000 records and is projected to increase by 30,000 by the end of 1980. Similar increases are anticipated for succeeding years.

B. Inventory and Audit

Current computer inventory listings are produced from the TSCADS data base for all 49 component Top Secret Control points. These listings form the basis for conducting annual inventories of all Top Secret documents. Once the inventories are completed an audit of all control points must be conducted to insure compliance with existing regulation and correct noted deficiencies.

C. Training and Program Development

Training of Area Top Secret Control Officers (ATSCOs) is a mandatory requirement if the TSCADS program is to proceed on a consistent and uniform basis throughout the Agency. Due to continuous personnel turnover of ATSCOs, training of new personnel becomes a full-time program vital to TSCADS success. Coupled with this training is the requirement to maintain and update the Top Secret Control Manual. Changing technology requires that the manual address the variety of ways in which TS documents are being created and reproduced.

Finally, the program development function of this Branch recognizes the need to continuously develop enhancements to the TSCADS software resulting in more efficient input and utilization of data.

III. Industrial Systems Branch

Information systems security is an integral part of the overall industrial security package at contractor locations, and the increased utilization of information systems to process and/or store Agency data increases our responsibility to insure that this data is adequately protected. Based on the current utilization and expected growth of contractor ADP systems, ISSG anticipates a continuous and increasing demand upon its assets in order to respond to official requests for computer security support.

Existing systems utilized by contractors are constantly being reconfigured while the number and complexity of new systems continue to increase. Contractors now desire to process in a multicompartmented mode to obtain maximum utilization of their ADP resources. Distributed processing (or networking) will also become an area of considerable security concern as contractors begin to express further interest in the use of these systems. These changes require continuing contact with the contractors and more frequent and time consuming on-site inspections to insure the security of Agency information.

STAT

IV. Agency and Community Systems Branch

The information systems security responsibilities of this Branch will focus upon three specific types of systems which are currently resident at Agency domestic locations:

A. Major Agency Internal Systems

These are the large information systems such as GIMS, VM, Batch/JES III and ALLSTAR which are accessible only by personnel cleared to Agency staff standards. They are internal to the Agency in that these systems are not connected to or shared with any other Community systems. By volume these systems contain the majority of data processed within the Agency. The systems are complex and are constantly undergoing hardware and software changes in order to meet user requirements. Providing security support to these systems in the form of developing effective auditing, accountability and data separation controls can only be done on a continuing basis and with sufficient manpower. These systems will continue to grow, change and be a major part of the Agency's data processing operations. In future years, the Office of Security will need to assign additional resources to these systems if we are to meet our regulatory responsibilities.

B. Community Systems

These are information systems physically located at Agency controlled buildings but available for access by other Community members via remote processing facilities.
STAT Examples of these systems are found at NPIC and [redacted] other examples are the CAMS and SAFE systems. These systems represent a growing trend in the Community; a resource sharing of equipment and data among Community members. Such systems require the same security protection and concern afforded to the major Agency internal systems. In fact, additional care must be taken to insure that the Community and internal Agency systems are not networked until or unless sufficient technology is developed to insure separation and control of data.

C. Agency Standalone Systems

These systems consist of hardware equipment that is used solely by one Agency component, does not share resources, and is not hardwired (linked) to another automated data processing system. The Office of Data Processing advises there are now 125 standalone systems in the Agency, and anticipate an annual increase of 20% over the next five years. Responsibility for these systems include security survey, assessment and approval for operation. While these systems are not as difficult to assess as a major shared system, they are subject to frequent changes in the hardware and software configurations, causing a need for frequent review and assessment.

V. Overseas Systems Branch

Information Systems Security Group must continue to establish policy and procedures and provide advice and guidance concerning the numerous complex issues involved in placing automated data processing equipment in field installations. Particular emphasis must be given to DDO overseas locations. In addition to establishing policy and procedural guidelines, ISSG must make a detailed assessment of each system environment prior to granting security approval. ISSG is heavily involved in the DDO Craft System and the Office of Finance Class A system, both of which involve processing Agency classified data at overseas locations.

ADP equipment for CRAFT and CLASS A will be placed at overseas stations and bases by 1981. Within the next five years, the CRAFT project anticipates that information processing equipment, including computers, remote terminals and word processors, will be located at STAT bases. Because computer technology is so dynamic, these systems will be constantly undergoing upgrading to more sophisticated equipment and software. Having knowledgeable individuals available on-site to assess the computer security vulnerabilities and provide advice and guidance will insure protection of Agency data. Assignment of these ISSOs at regional locations in Europe, Asia and Africa will insure prompt information systems security support to overseas stations and bases.

Overseas assignment of ISSG personnel will be in addition to a certain number of ISSOs assigned to CRAFT at Headquarters. Current plans, pending EXCOM approval, call for assignment of one full-time ISSO in FY 1981, and two additional ISSO's in FY 1982.

VI. Policy and Program Development Branch

The primary mission of this Branch is to formulate and propagate the many policy decisions in the information systems security field in concert with related Agency and Intelligence Community policies. Additional responsibilities of this Branch relate to providing support to the other Branches of ISSG. This support consists of training and briefing; providing technical support and guidance, and developing and administering contracts to further the overall programs of ISSG. As the other Branches continue to expand in their functions and responsibilities, the Policy and Program Development Branch must also expand.

A. Training

The policy propagation function is performed by a training section which is structured to provide computer security instruction for all major ODP and OTR data processing training courses as well as for other groups as the need arises. The training section would publish, on a regular basis, notes and guidelines on subjects of computer security for distribution to data processing personnel and users. The Training section would also monitor the internal training for ISSG personnel, so that they can continually improve and update their knowledge of data processing and information systems security.

B. Liaison

The coordination of the policy is done through the Liaison section of the Branch which is a primary participant in a number of Agency and Interagency committees which have information systems security responsibilities. Increased technology in upcoming years will place additional pressures to continue developing realistic policies.

C. Contract Development and Administrative/Engineering and Technology Sections

Another mission of the Branch is to promote promising new initiatives, technical and procedural, to further the

overall programs of ISSG. This mission would be conducted by a Contract Development and Administrative Section in coordination with an Engineering and Technology Section. These sections would explore new developments of potential value in the information security field. They would do this through liaison with the R&D components of this and other agencies; through self-initiated contacts with industry, and through review of publications. They would also be responsive to the expressed requirements of the other ISSG Branches in the formulation of contracts.

The Contract Development and Administrative Section would monitor technical contracts and personal services contracts for consultants.

An additional responsibility of the Engineering and Technology Section will be to provide technical advice and guidance in support of the other Branches of ISSG.